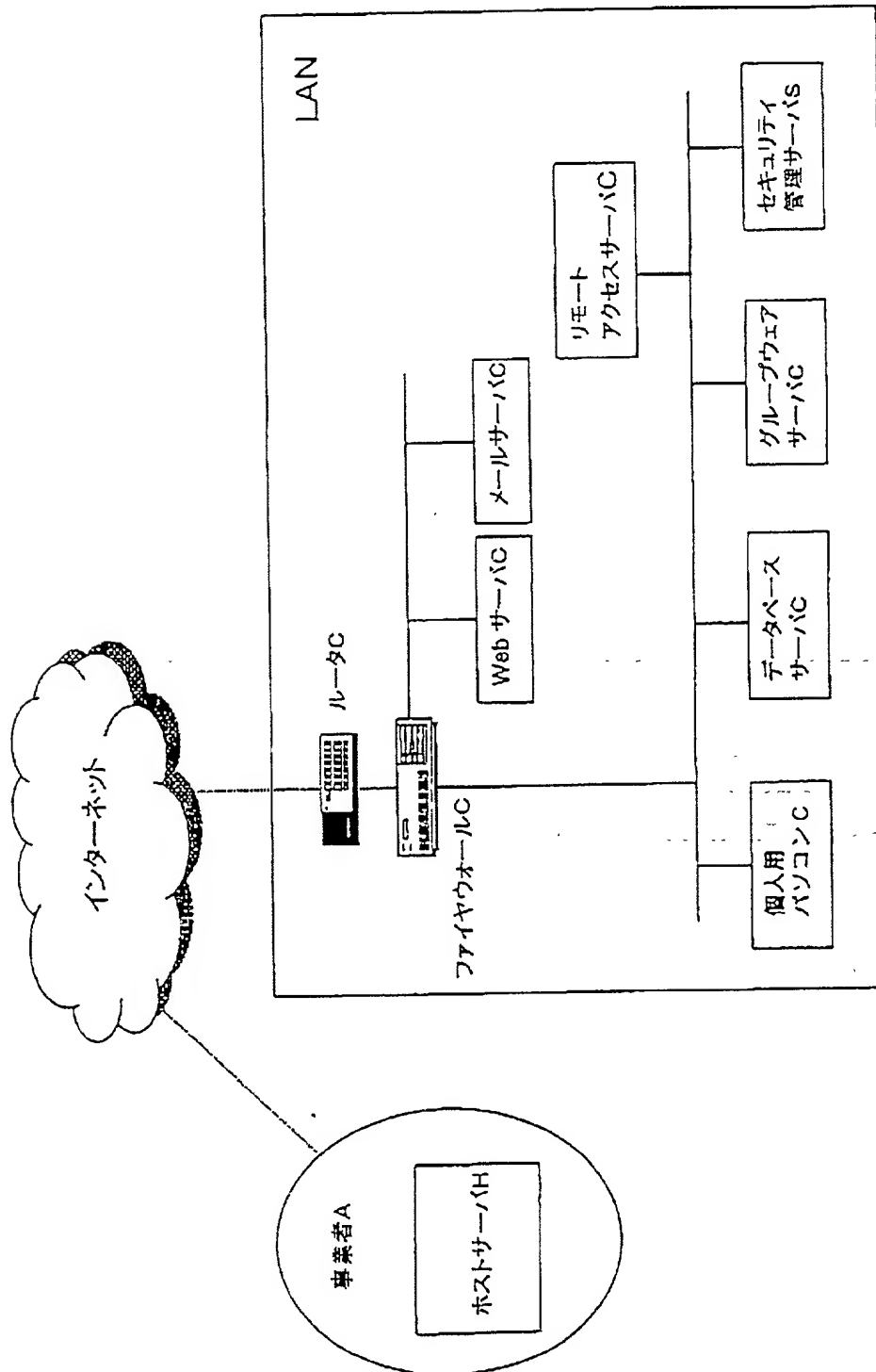


提出日 平成13年 6月 5日
頁: 1/ 21

発明番号 = ID010220

【書類名】 図面

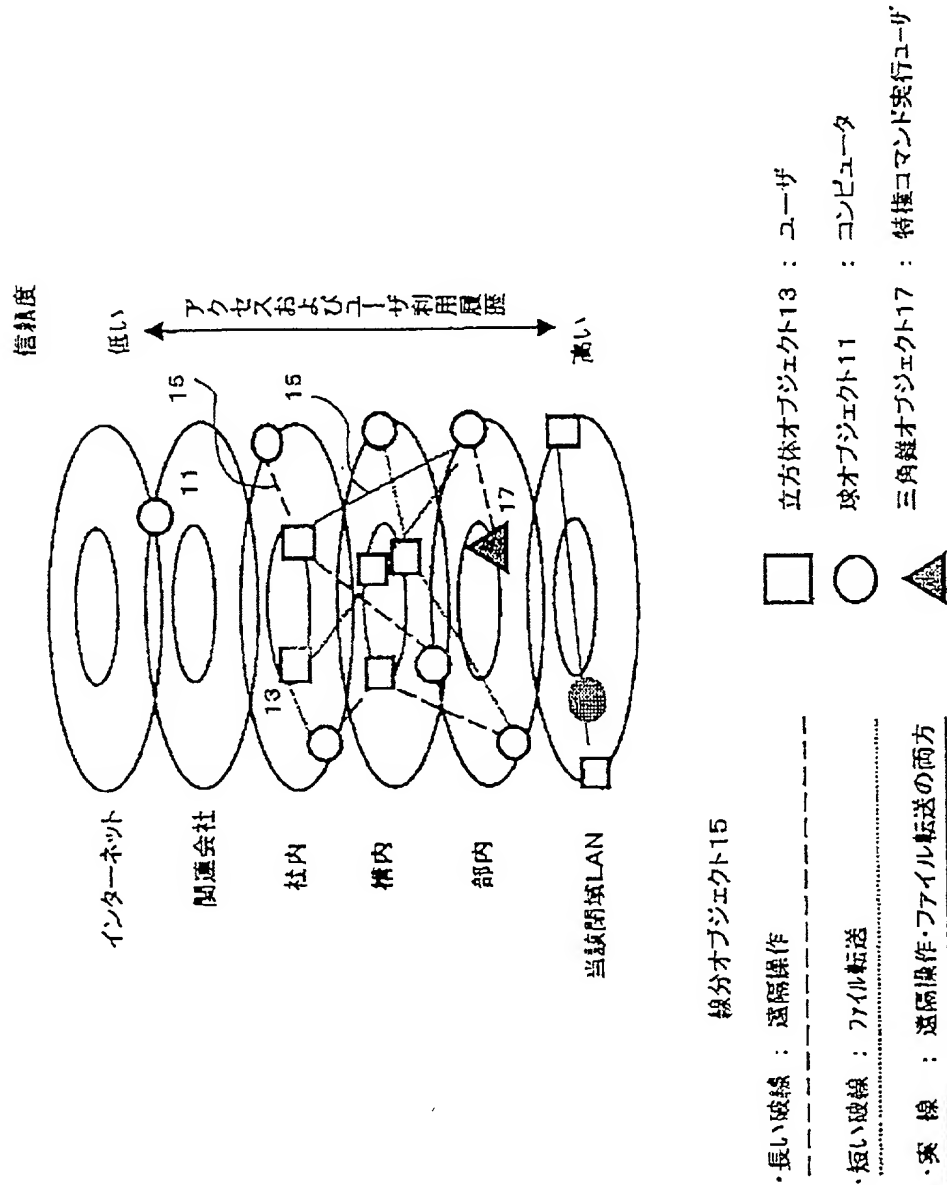
【図1】



提出日 平成13年 6月 5日
 頁: 2/ 21

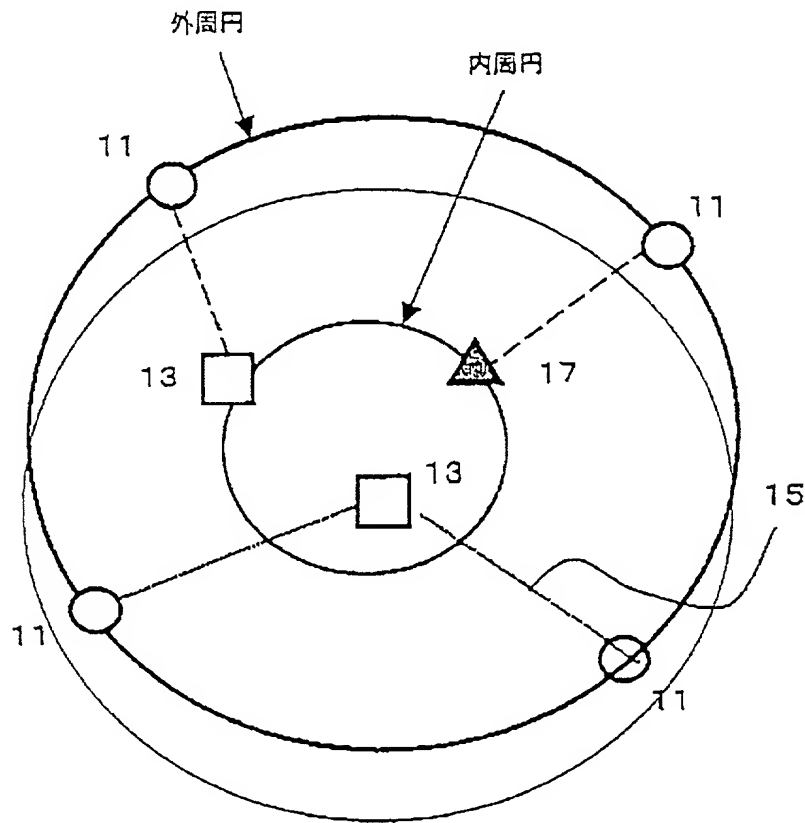
整理番号=ID010220

【図2】



整理番号=ID010220

【図3】



提出日 平成13年 6月 5日
 頁: 4/ 21

特許番号 = ID010220

【図4】

| 対象装置 | レイヤーの表示方法(グループ分け) | | | | 表示時間 | | 表示内容 | |
|-------------|-------------------|------|-------|---------|--------|-----------|--------|------|
| | ドメイン別 | 部門別 | ビル棟層別 | アクセス種別 | リアルタイム | プレイバック | デフォルト | 任意 |
| 1 個人用パソコン | | | ○ | | ○ | | | ○ |
| 2 データベースサーバ | | | | ○ | ○ | | | ○ |
| 3 Webサーバ | ○ | | | | ○ | | ○ | |
| 4 メールサーバ | | ○ | | | | ○ | ○ | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| 10 | | | | | | | | |
| 環境設定 | OS | | | | DHCP通信 | | ログ収集時間 | |
| | unix | unix | unix | Windows | OPEN | SEER DHCP | 5分 | 任意 |
| 1 個人用パソコン | ○ | | | | | ○ | ○ | |
| 2 データベースサーバ | ○ | | | | | ○ | ○ | |
| 3 Webサーバ | | | ○ | | ○ | | ○ | 240分 |
| 4 メールサーバ | | | ○ | | ○ | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| 10 | | | | | | | | |

整理番号=ID010220

頁: 5/ 21

【圖5】

| | 21 | 22 | 23 | 24 |
|--|----|----|----|----|
| Jun 25 01:11:08 comp1 syslogd: restart Jun 25 03:26:50 comp1 fipd[28955]: connection from kawa.yama.ucc.ac.jp as mana Jun 25 03:27:00 comp1 fipd[28955]: FTP LOGIN FROM kawa.yama.ucc.ac.jp as mana Jun 25 03:40:00 comp1 fipd[28955]: no rw ds lls system in mlab Jun 25 03:00:00 comp1 fipd[28974]: tar -xzf -m/acc/mstab -t 7800 -f /vrbtmp. Jun 25 03:30:30 comp1 Xsession: minsta; login Jun 25 05:16:03 comp1 fipd[28973]: connection from kawa.yama.ucc.ac.jp Jun 25 06:14:33 comp1 fipd[28973]: FTP LOGIN FROM kawa.yama.ucc.ac.jp as mana Jun 25 06:37:52 comp1 Xsession: minsta; logout Jun 25 19:48:18 comp1 login[31071]: ? at curpr.yama.ucc.ac.jp as oymlba Jun 25 21:13:26 comp1 nls: WARNING: AFP: got MAC address Jun 25 21:14:10 comp1 Xsession: minsta; login Jun 25 21:30:49 comp1 fipd[31005]: connection from kawa.yama.ucc.ac.jp Jun 25 03:48:18 comp1 fipd[31005]: FTP LOGIN FROM kawa.yama.ucc.ac.jp as mana Jun 25 03:42:18 comp1 fipd[31003] Jun 25 01:11:05 comp1 Jun 25 02:26:58 comp1 Jun 25 02:28:58 comp1 Jun 25 03:00:05 comp1 Jun 25 03:00:05 comp1 Jun 25 03:20:38 comp1 fipd[28974]: tar -xzf -m/acc/mstab -t 7200 -f /vrbtmp. Jun 25 04:15:03 comp1 Xsession: minsta; login Jun 25 05:16:03 comp1 fipd[28973]: connection from kawa.yama.ucc.ac.jp Jun 25 05:22:02 comp1 Xsession: minsta; logout Jun 25 19:48:18 comp1 login[31071]: ? at curpr.yama.ucc.ac.jp as oymlba Jun 25 21:14:10 comp1 Xsession: minsta; login Jun 25 21:30:49 comp1 Xsession: minsta; logout Jun 25 03:42:18 comp1 fipd[31005]: connection from kawa.yama.ucc.ac.jp Jun 25 03:42:18 comp1 fipd[31003] | | | | |

提出日 平成13年 6月 5日
 頁: 6/ 21

整理番号=ID010220

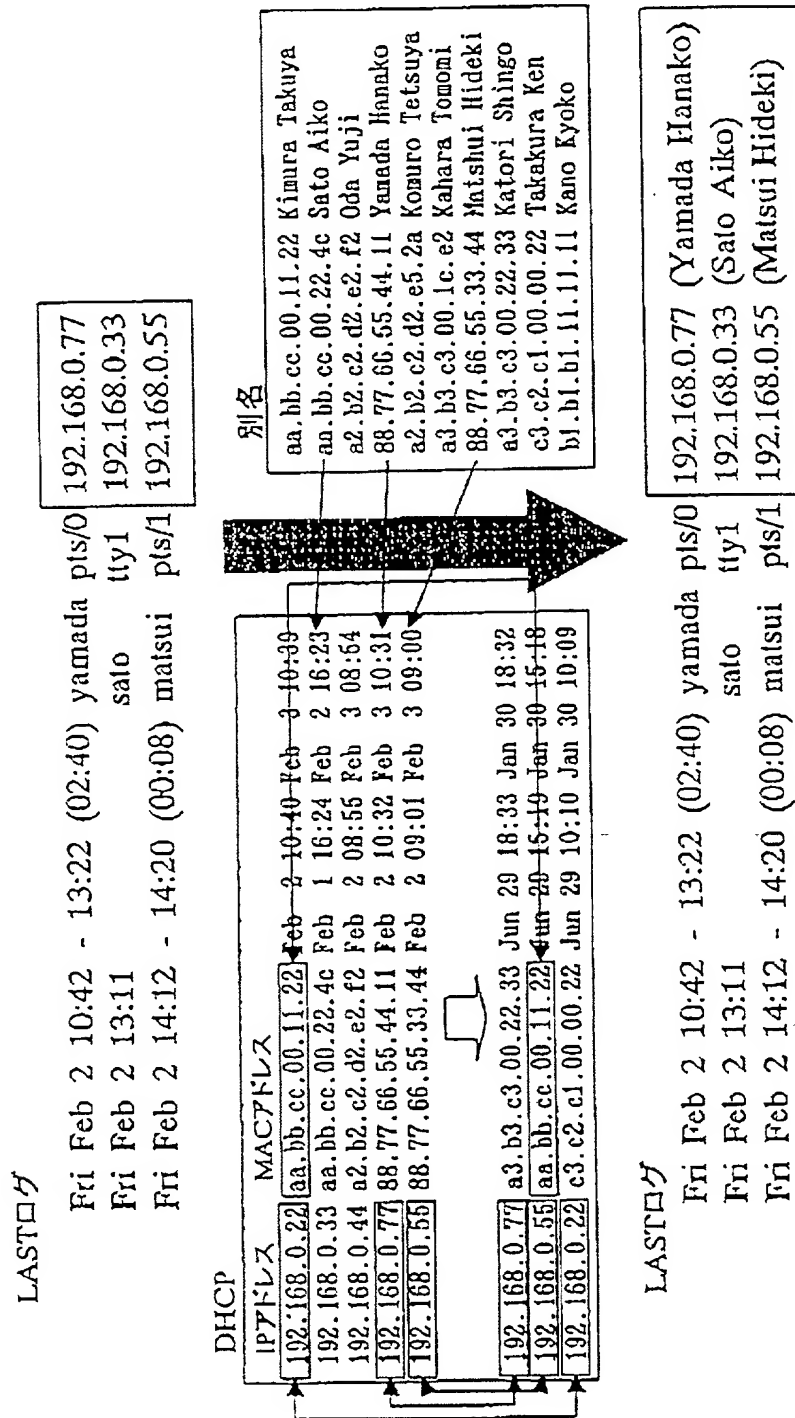
【図6】

| | | | | | | |
|------------|-------------|----------|-------------|---------|---------------|--------|
| | 〇〇〇株式会社 | | CSO：向井 徹 | | システム管理者：足立 正浩 | |
| 管理対象コンピュータ | | スペック | サービス内容 | | | |
| | | | 基本機能 | 3D描画化 | リモート監視 | ログ閲覧 |
| 1 | DBSサーバ1 | Solar | ○ | ○ | ○ | ○ |
| 2 | DBSサーバ2 | Solar | ○ | ○ | ○ | ○ |
| 3 | Webサーバ1 | Linux/IC | ○ | ○ | ○ | ○ |
| 4 | Mail | Linux/IC | ○ | ○ | ○ | ○ |
| 5 | RAS Gateway | Solar | - | ○ | - | ○ |
| 6 | | | | | | |
| 7 | | | | | | |
| ● | 管理サーバの稼働状況 | | | | | |
| 稼働状況 | | 設置場所 | 管理対象コンピュータ | | | |
| | | | 1 | 2 | 3 | 4 |
| 1 | 正常 | 社長室 | DBSサーバ1 | DBSサーバ2 | Webサーバ | メールサーバ |
| 2 | 正常 | 情報管理室 | リモートGateway | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

提出日 平成13年 6月 5日
頁: 7/ 21

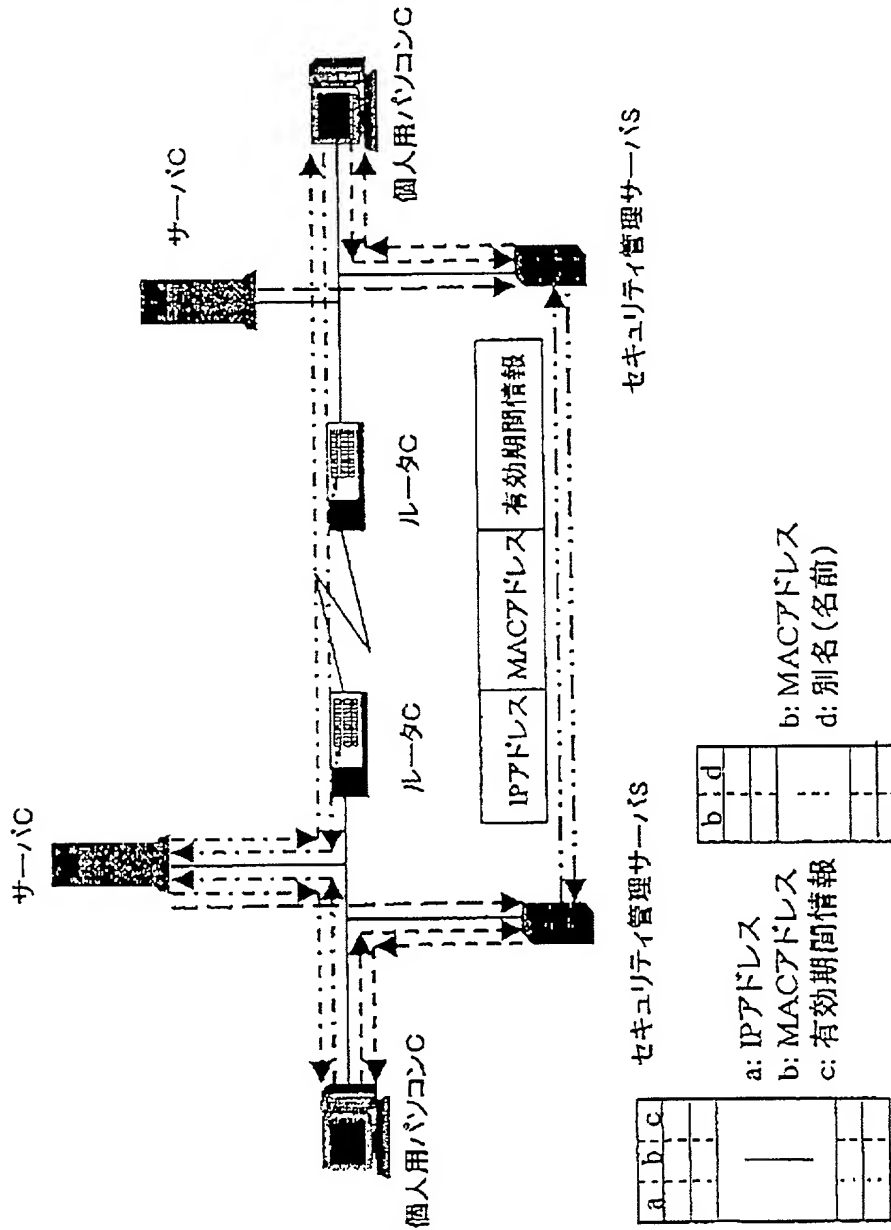
整理番号=ID010220

【図7】



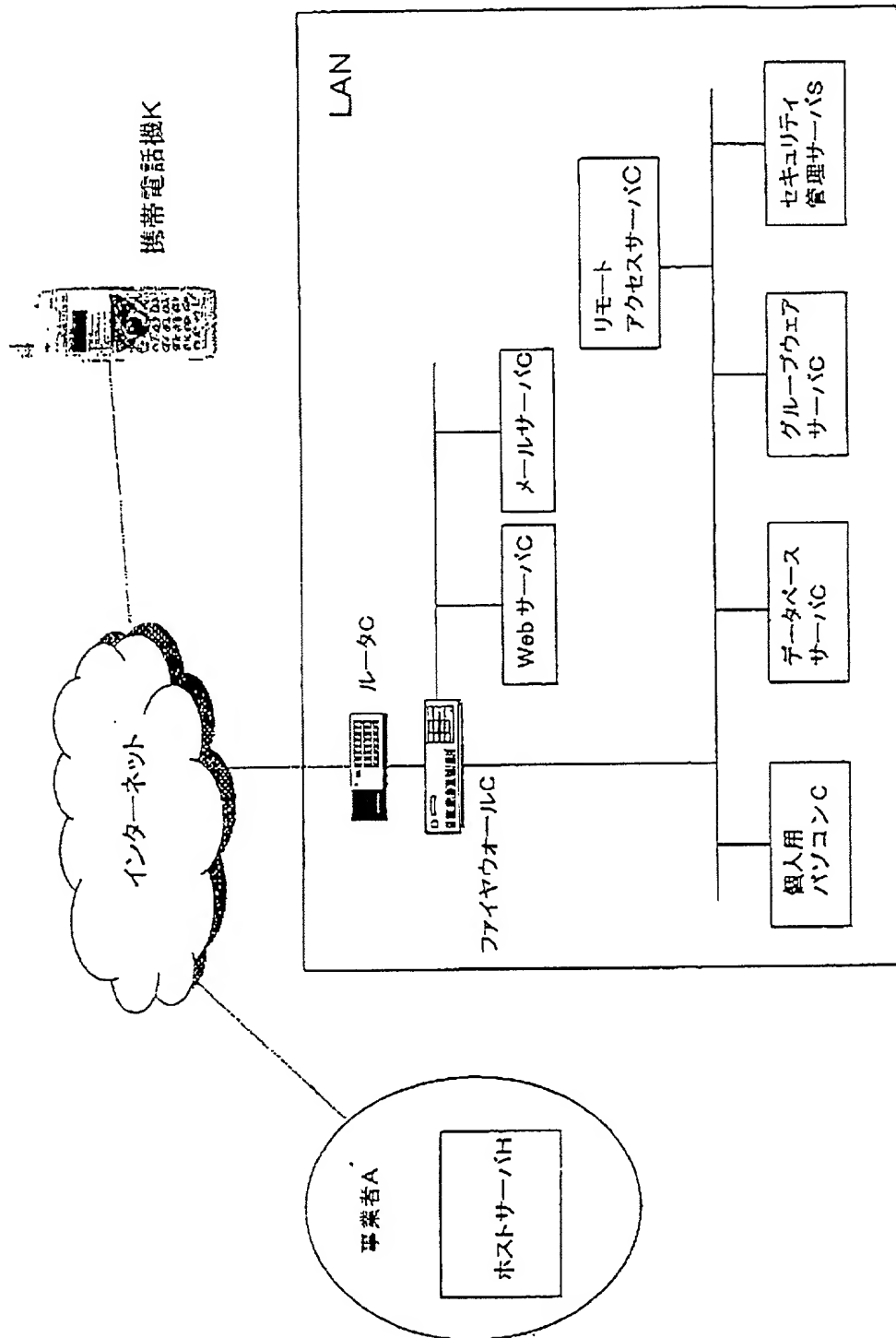
整理番号=ID010220

【図8】



整理番号=ID010220

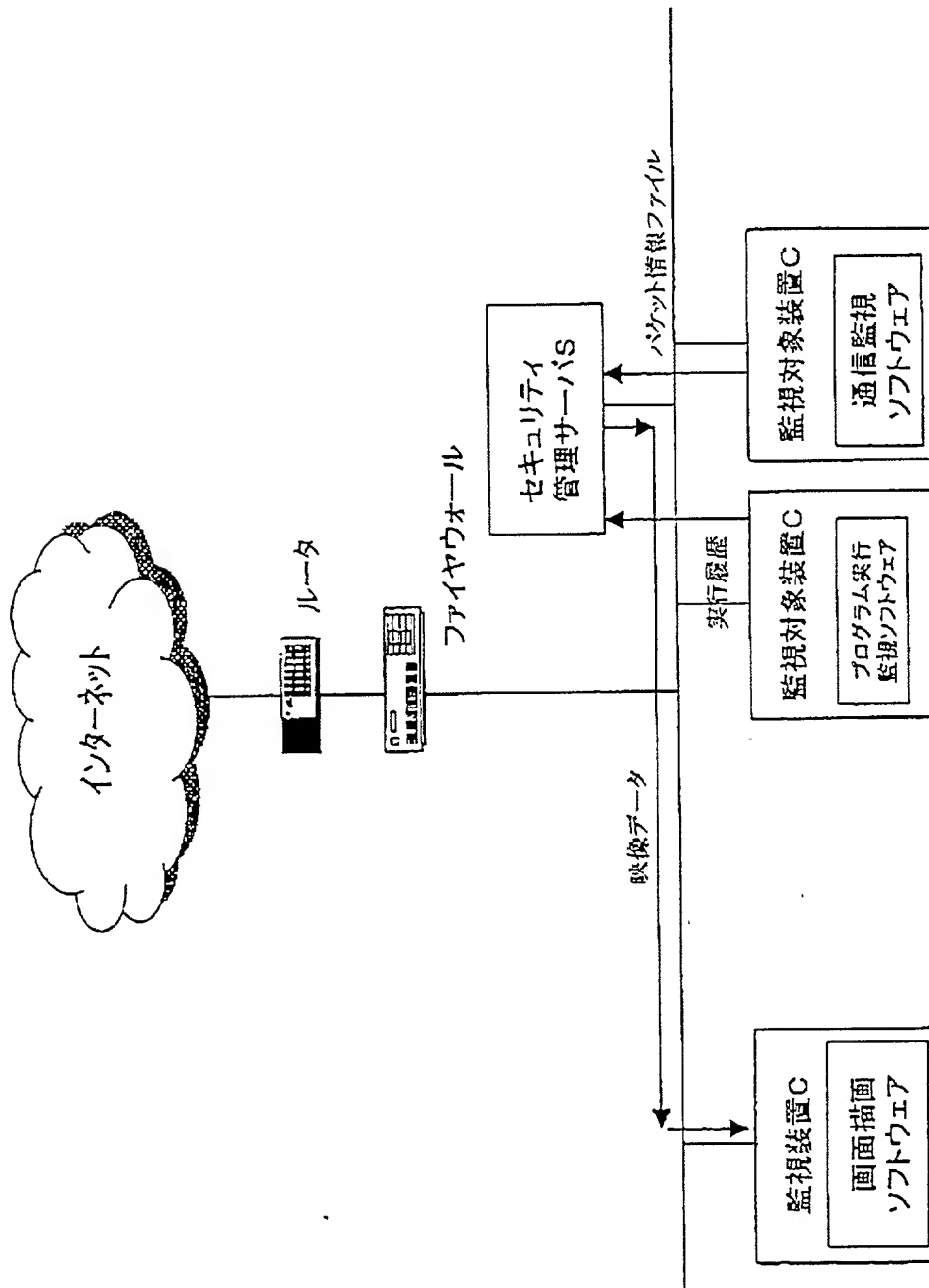
【図9】



提出日 平成13年 6月 5日
頁: 10/ 21

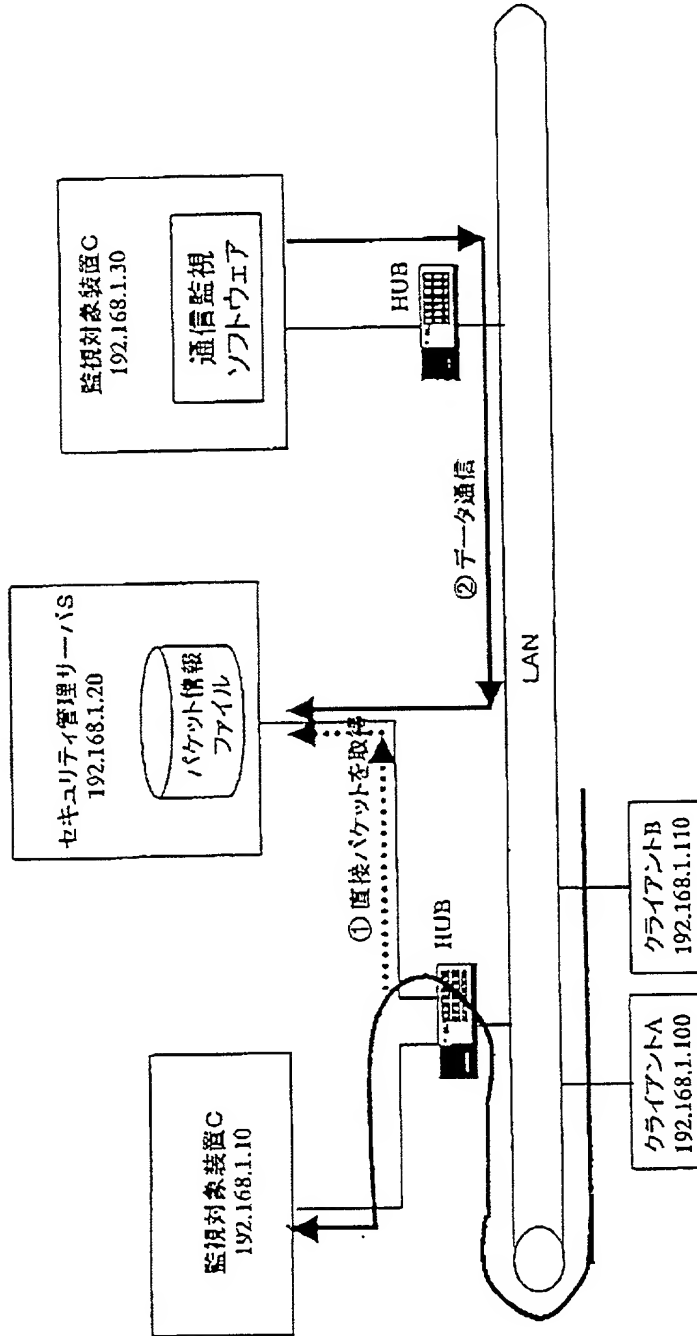
整理番号=ID010220

【図10】



整理番号=ID010220

【図11】



- ① セキュリティ管理サーバSと同一HUBに接続されている監視対象装置Cの通信パケットは直接取得可能
- ② セキュリティ管理サーバSと異なるHUBに接続されている監視対象装置Cの通信パケットは、監視対象装置C側で蓄積記憶しておき、これをLAN経由のデータ通信により適宜セキュリティ管理サーバSに送信する。

提出日 平成13年 6月 5日
頁: 12/ 21

整理番号=ID010220

【図12】

パケット情報ファイルのデータフォーマット

| フィールド名 | 説明 |
|--------------|---|
| time | 収集時間(サーバー時間) |
| btFlags | フラグ 0:IN 1:OUT (サーバーから見て) 2:SMB(共有ファイルアクセス等) |
| wLength | パケットのオリジナル長 |
| mwMac | クライアント MAC アドレス |
| dwIPAddr | クライアント IP アドレス |
| wPort | サーバーポート番号 |
| btDataLength | パケットの可変データ部分の長さ (0から255) |
| btData[256] | 256パケットの可変データ(可変長) |

【図13】

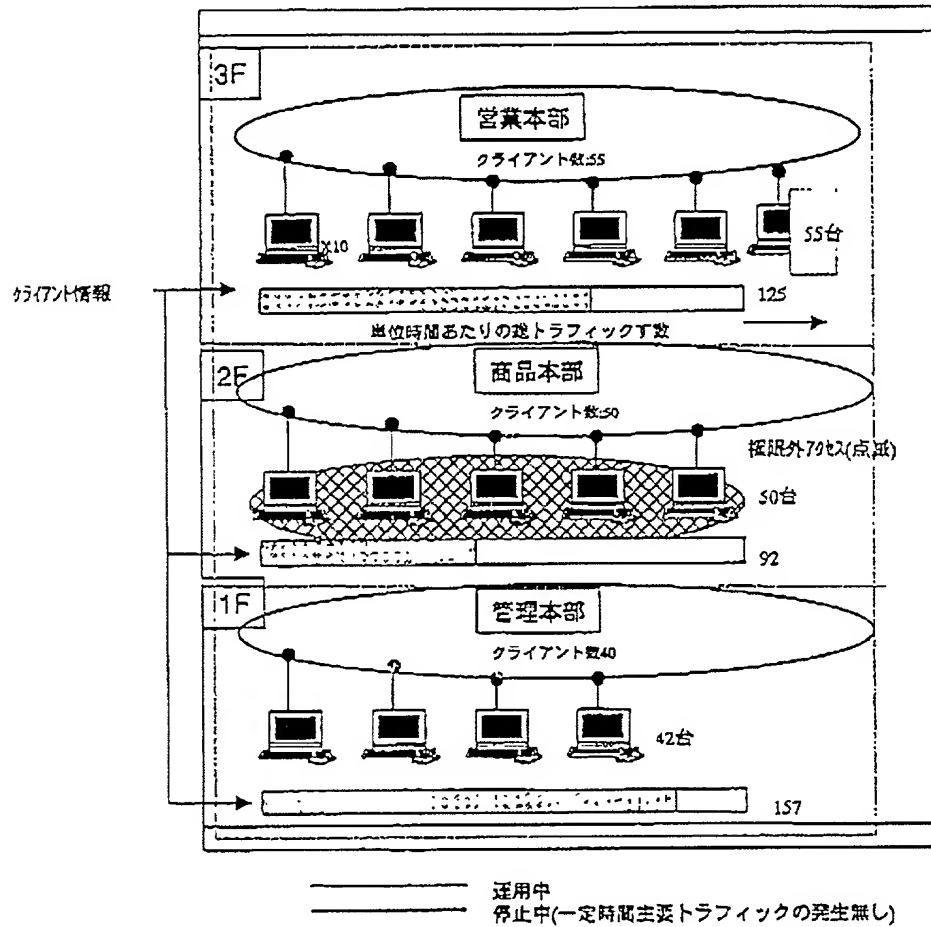
視覚化基礎データ

| フィールド名 | 説明 |
|-----------------|---|
| time | 収集時間(セキュリティ管理サーバでの時間) |
| wServerID | 監視対象サーバー識別子 |
| wType | パケットのタイプ (01:Login...65:Mail...) |
| mwMac | クライアント MAC アドレス |
| dwIPAddr | クライアント IP アドレス |
| wOriginalLength | パケットのオリジナル長 |
| btData[256] | 256パケットのタイプ別文字データ (Login:UserID/Mail:from.to...) |

提出日 平成13年 6月 5日
頁: 13/ 21

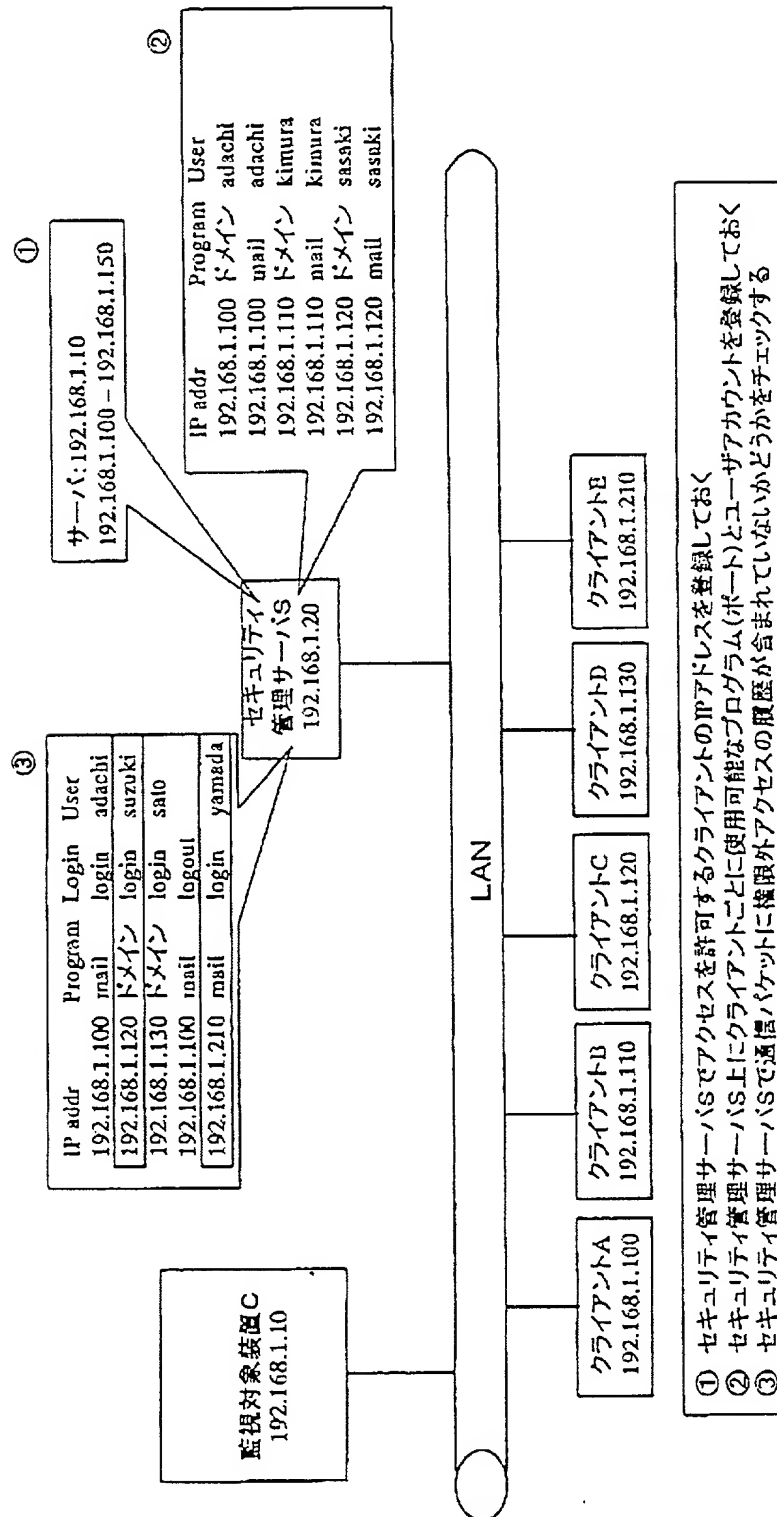
整理番号=ID010220

【図14】



整理番号=ID010220

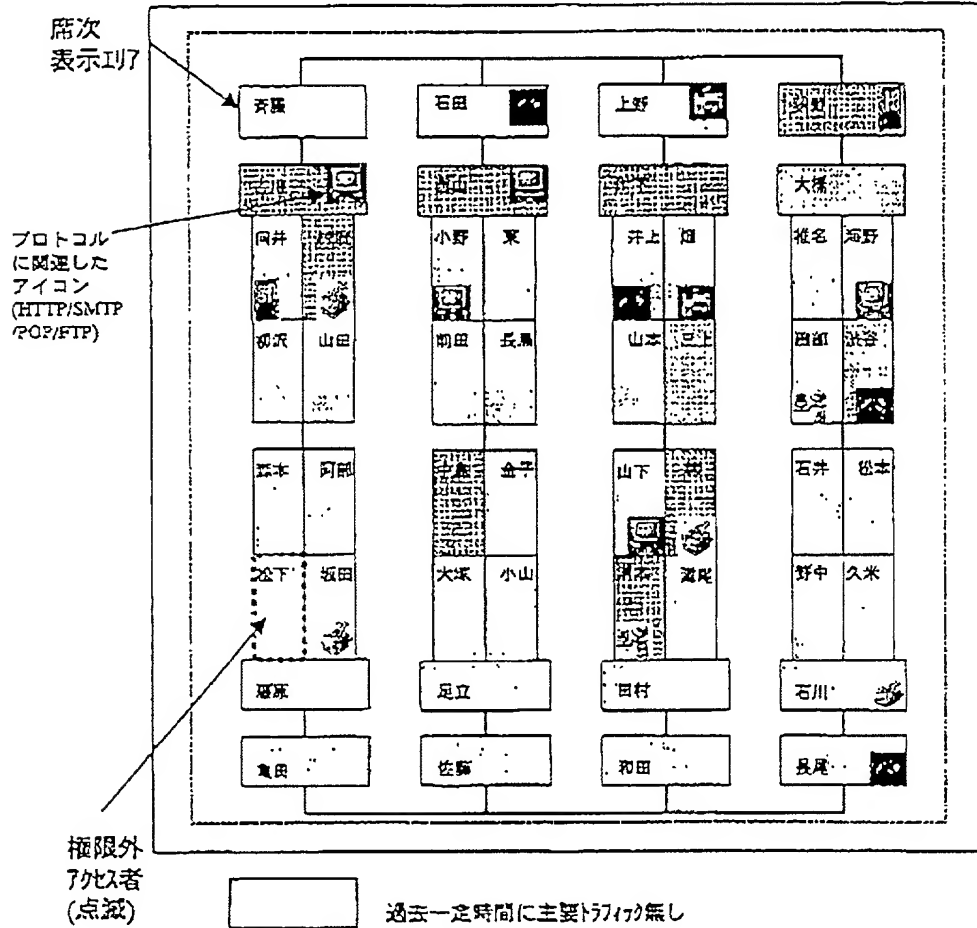
【図15】



提出日 平成13年 6月 5日
 頁: 15/ 21

整理番号=ID010220

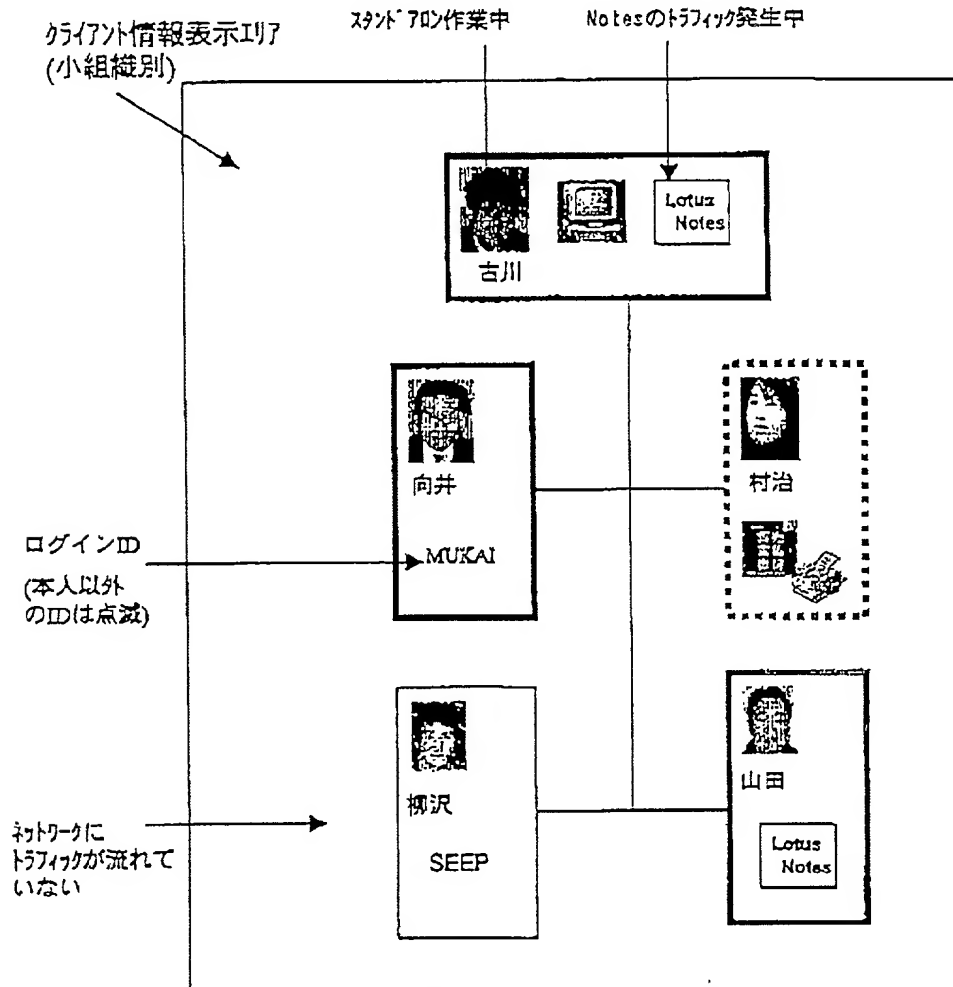
【図16】



提出日 平成13年 6月 5日
頁: 16/ 21

整理番号=ID010220

【図17】




提出日 平成13年 6月 5日
 頁: 17/ 21

発通番号 = ID010220


【図18】

クライアント情報画面

利用者: Senri Yamada



スタイル:



ユーザ情報:





















| | | | | | | | |
|---------|---------------------------------------|------|------|------|---------|-----|----|
| 氏名: | 山田 千鳥 | 所属1: | 営業本部 | 所属2: | 金融商品企画部 | 性別: | 男性 |
| IPアドレス: | 201.10.161.89 E-mailアドレス: yamada@seec | | | | | | |

システム情報:

| | | | | | |
|-------------|-------|--------|----------|--------|-------------|
| 情報カテゴリ: | Notes | 管理管理方法 | 市場平価システム | バージョン: | Office 2000 |
| 利用アプリケーション: | 顧客DB | 取引先DB | 人事DB | | |
| 100利用権限: | 3:閲覧 | 2:更新 | 4:部分閲覧 | | |

利用情報

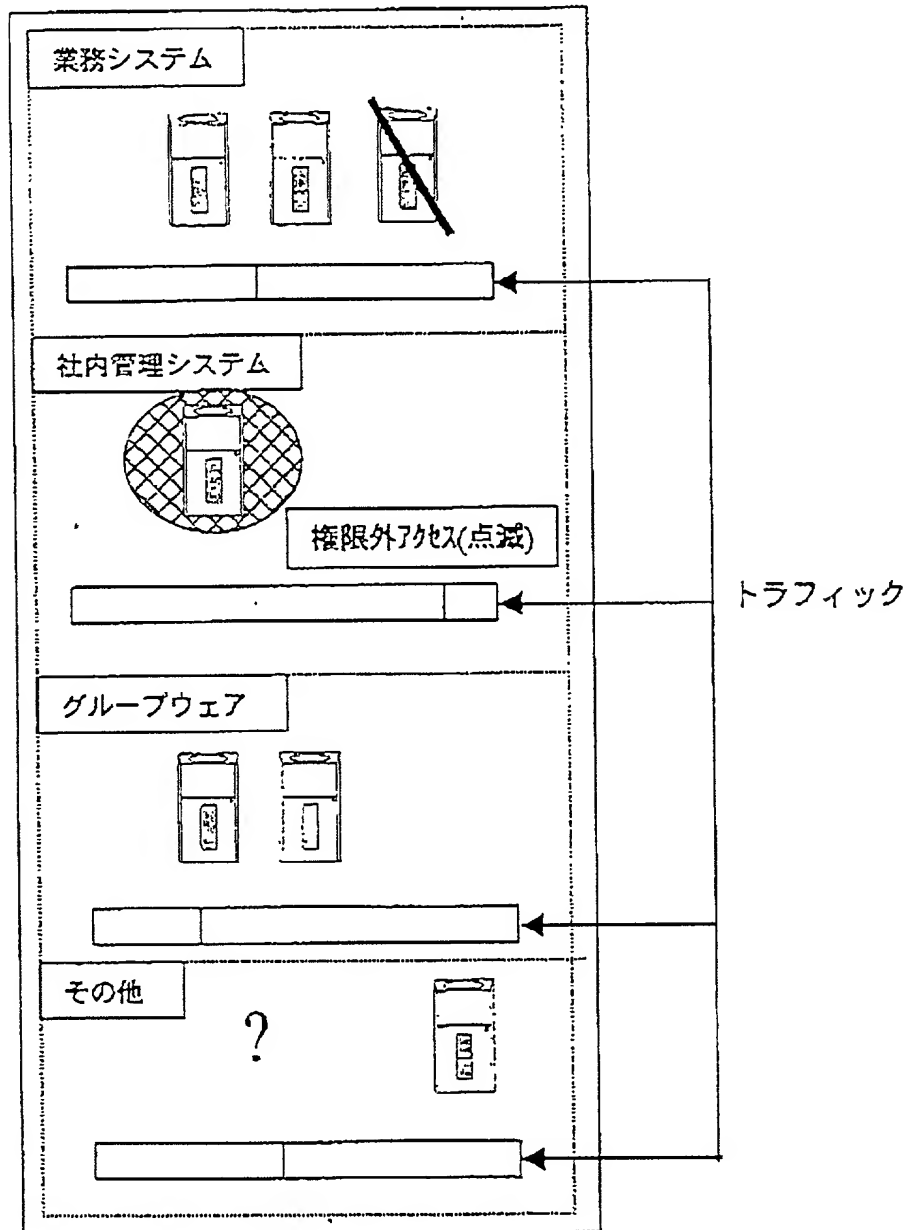
☐ 過去1時間
 ☒ 本日履歴
 ☐ 月
 ☐ 日
 ☐ 履歴

| | | | | |
|---|--|---|---|--|
|  ネットワーク 設定 |  内用Web ツール |  E-Mail |  業務システム |  その他 |
|  ネットワーク 設定 |  内用Web ツール |  E-Mail |  業務システム |  その他 |
|  ネットワーク 設定 |  内用Web ツール |  E-Mail |  業務システム |  その他 |
|  ネットワーク 設定 |  内用Web ツール |  E-Mail |  業務システム |  その他 |

提出日 平成13年 6月 5日
頁: 18/ 21

整理番号=ID010220

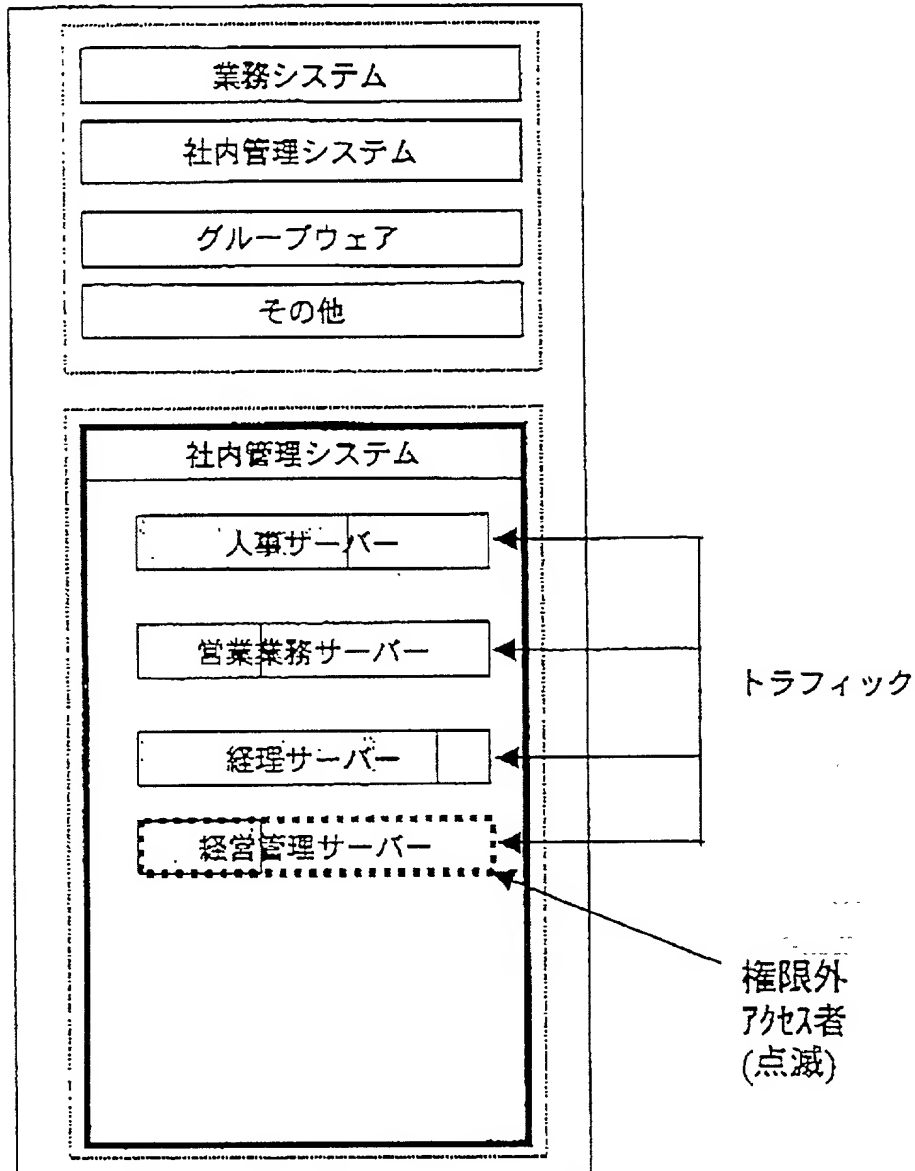
【図19】



提出日 平成13年 6月 5日
頁: 19/ 21

整理番号=ID010220

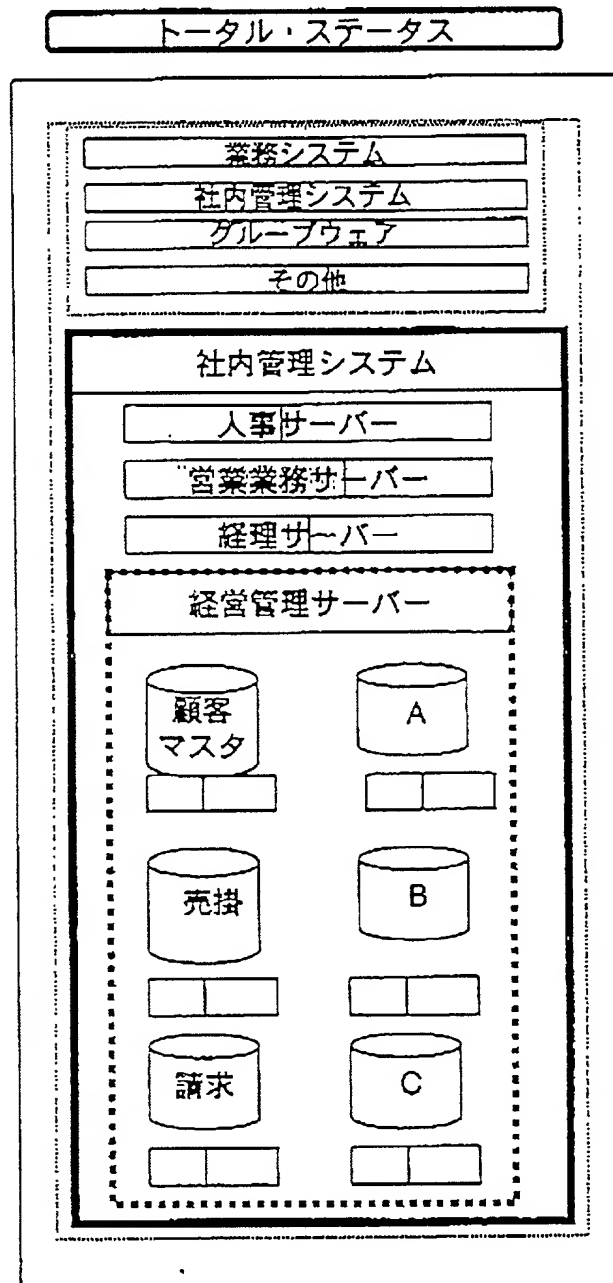
【図20】



提出日 平成13年 6月 5日
頁: 20/ 21

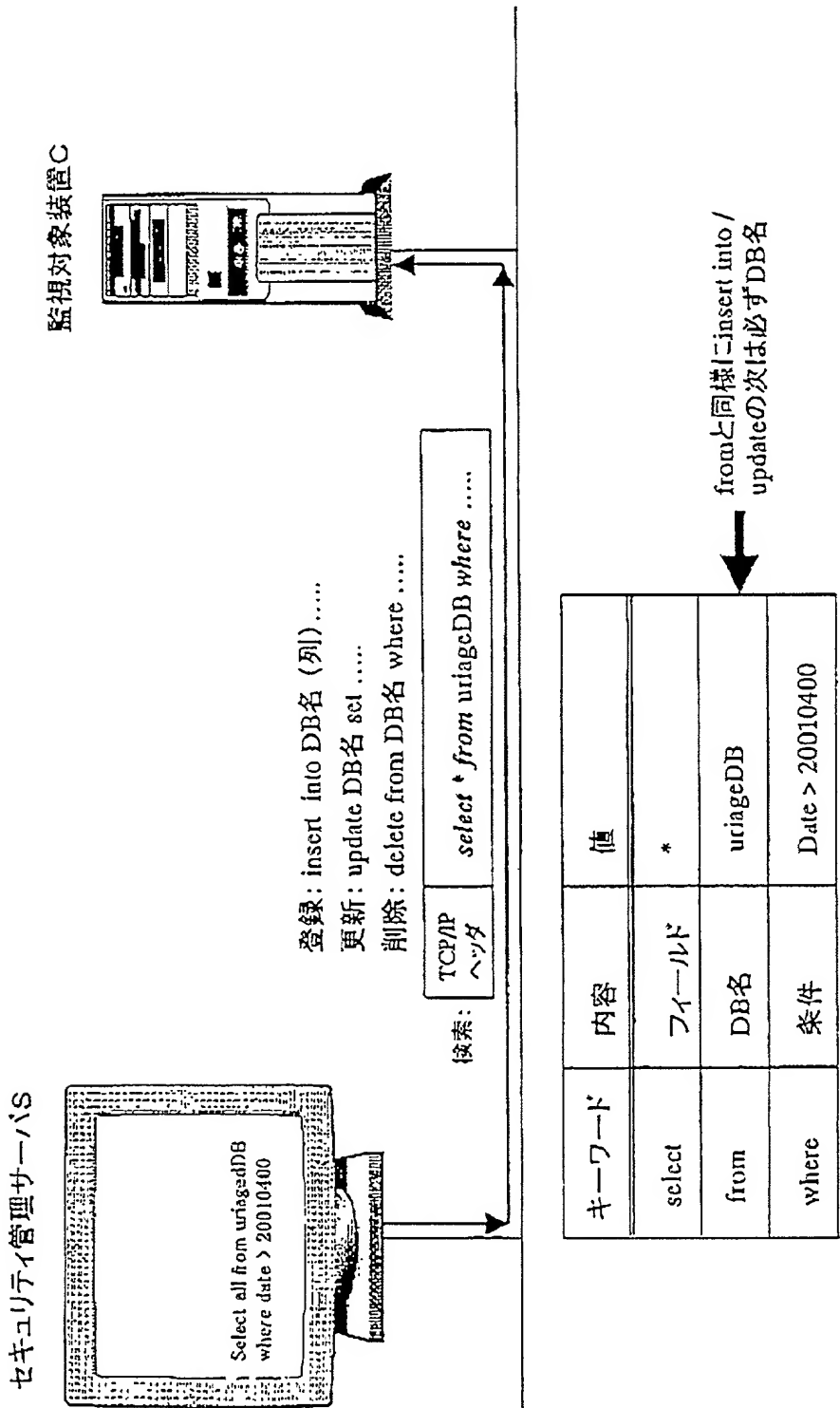
整理番号=ID010220

【図21】



整理番号=ID010220

【図22】



提出日 平成13年 6月 5日
頁: 1/ 1

整理番号=ID010220

【書類名】 要約書

【要約】

【課題】 LANにおける各種のセキュリティサービスを提供するセキュリティ管理サーバおよびこれと連携して動作するホストサーバを提供する。

【解決手段】 インターネットなどの外部のネットワークに接続するLAN内に、LAN内で稼働する各種監視対象装置C内で管理されている各種のログ情報を収集する機能、収集したログ情報からLANのセキュリティ管理に有用な情報を抽出してこれを人が利用しやすい形態に視覚化した映像を生成する機能、前記映像を他の監視装置Cに送信する機能を備えたセキュリティ管理サーバSを設置する。また、セキュリティ管理サーバSは、外部のネットワークで稼働するホストサーバHと連携して各種のセキュリティサービスを提供する。

【選択図】 図1